

Administración de Sistemas GNU/Linux PEC3

Lic. Fausto Mauricio Lagos Suárez

30 de mayo de 2012

1. Parte 1: Reflexión

Para la implantación requerida se sugiere cumplir con la siguiente configuración de hardware y software:

1. **Hardware:** Adquirir tres discos duros SATA III Western Digital Caviar Green de 3 TB cada uno a un costo de 128,39 Euros y un disco duro Western Digital Caviar Green SATA III de 2 TB con un costo de 90,63 euros, lo que implicará un inversión total de 475,8 Euros.

La elección del fabricante de los discos, relativa a la calidad esta soportada en pruebas comparativas¹ entre discos similares de la misma línea de Western Digital, Samsung y Seagate en cuyos resultados Western Digital muestra ser superior que sus competidores en rendimiento, tiempo de respuesta, consumo (característica de la serie Green), temperatura de trabajo entre otras características analizadas, además la diferencia en precios no es muy significativa para preferir la superioridad en características propias del dispositivo.

Respecto de la cantidad de discos sugeridos para ser adquiridos se presenta el diagrama de configuración a continuación.

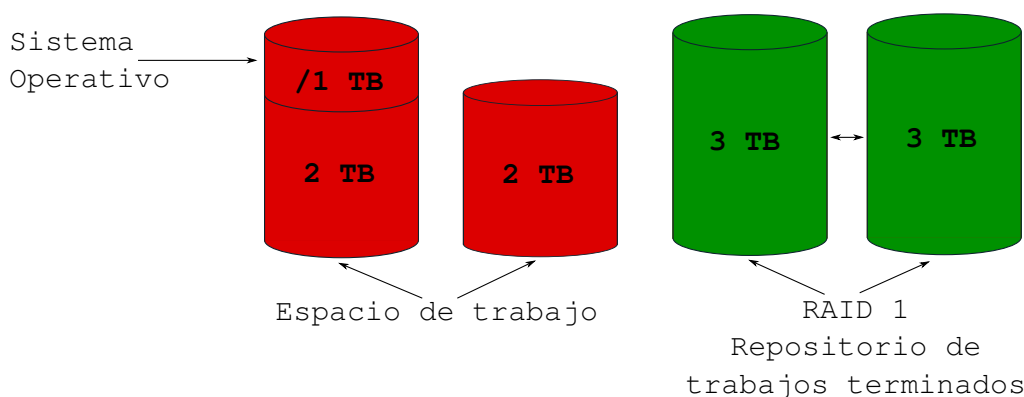


Figura 1: Distribución del espacio de almacenamiento

El espacio de trabajo se configura en un volumen lógico en RAID 0.

Se adquirirán los discos indicados con estas capacidades dado que en el mercado no es fácil encontrar capacidades superiores y además esta en discusión el soporte del hardware adquirido así como la configuración del software para que capacidades superiores puedan

¹<http://hothardware.com/Reviews/Definitive-2TB-Hard-Drive-Roundup/?page=1>

andar sin problemas, 3 TB es una capacidad que ya esta suficientemente testada tanto con dispositivos de hardware (placas base, memorias, etc) así como con sistemas operativos y software, la tecnología de 4 TB (con Western Digital como uno de los primeros en producirla) es relativamente nueva (Septiembre de 2011) y fabricantes como Seagate y el mismo Western Digital ofrecen más soporte para dispositivos de almacenamiento externo que interno.

2. **Software:** La distribución de GNU/Linux seleccionada se montará en una partición de 1 TB, el sistema operativo (Debian GNU/Linux) será montado en configuración de servidor de archivos, los 2 TB restantes de esa unidad, junto con la otra unidad de 2 TB serán montados en el mismo volumen lógico en RAID 0, como ya se mencionó los 4 TB deseados para las tareas de trabajo, y los dos discos de 3 TB serán montados en configuración RAID 1 que será montado en un punto definido específicamente para ello en la tabla de particiones.

2. Parte 2: Práctica CUPS

Para resolver esta parte se montón una máquina que se configuró como servidor de impresión, instalando y configurando el servidor CUPS, y dos máquinas clientes, una utilizando Debian GNU/Linux y otra Canaima GNU/Linux.

La configuración de los clientes CUPS se hizo creando el archivo client.conf, y editandolo como sigue:

```
cliente1# vi /etc/cups/client.conf

# ServerName - La dirección en la red, del servidor
ServerName 192.168.1.4

# Encryption - Requerimiento de encriptación
IfRequested
```

La configuración del servidor se hizo editando el respectivo archivo cups.conf en donde se resolvieron también las cuestiones indicadas en los siguientes numerales.

- a) *Habilitar la impresión desde cualquier máquina de la red local sin autenticar sobre la impresora.* Para lo cual en el archivo cups.conf se modificaron las siguientes líneas.

```
# Only listen for connections from the local machine
Listen *:631

# Show shared printers on the local network.
Browsing On
BrowseOrder allow,deny
BrowserAllow @LOCAL
```

Las anteriores modificaciones redundan en que el servidor escuche a cualquier máquina de la red local, teniendo en cuenta que la autenticación predefinida es Anonymous en lo que sería la directiva AuthClass, al escuchar todas las máquinas, todos los usuarios de la red podrán imprimir sin que deban autenticarse en la impresora, y con respecto a la sección de visualización de las impresoras de red, esa líneas aseguran que una máquina nueva en la red pueda ver y agregar la impresora compartida.

- b) *Teniendo en cuenta la dirección pública del servidor, habilitar la impresión por cualquier usuarios del sistema.* Se asignó permiso de acceso al servidor a todos los usuarios de la red

```
# Restrict access to the server...
<Location />
Order allow,deny
Allow localhost
Allow from all
</Location>
```

- c) *Permitir gestionar el servidor de impresión desde la dirección IP de la red (no sólo desde el localhost)* Nuevamente editando el archivos cupsd.conf

```
# Restrict access to the admins pages..
<Location /admin>
Order allow,deny
Allow from all
</Location>
```

Teniendo en cuenta que la modificación del archivo cupsd.conf hace parte de la administración del servidor de impresión, se habilitó también el acceso al archivo de cups.conf

```
# Restrict access to configuration files...
<Location /admin/conf>
...
Order allow,deny
Allow localhost
Allow from all
</Location>
```

- d) *Configurar para que el usuario Juan NO pueda imprimir en la impresora definida anteriormente.* Llamó la atención el hecho de que en el archivo cupsd.conf no existiera definida por defecto la sección /admin/printers que es donde se suponía deberá aparecer la denegación de servicio para el usuario Juan, se definió esta sección sin conseguir el resultado esperado con lo que desde la interface web del servidor sección Impresoras se consiguió denegar el servicio al usuario Juan.

PDF (inactiva, aceptando trabajos, compartida, predeterminada del servidor)

Mantenimiento Administración

Descripción: PDF
Ubicación: PEC3
Controlador: Generic CUPS-PDF Printer (color, dúplex)
Conexión: cups-pdf/

Opciones predeterminadas: job-sheets=none, none media=na_letter_8.5x11in sides=one-sided

Usuarios permitidos para PDF

Usuarios:

☐ Permitir a estos usuarios imprimir ☒ Evitar que estos usuarios impriman

Figura 2: Denegación del servicio al usuario Juan

Como soporte del funcionamiento del servidor en la siguiente imagen aparece parte del registro del servidor de los trabajos de impresión, en este registro pueden verse los tres usuarios de la red que han enviado trabajo a la impresora, en la parte posterior (abajo) del registro de trabajos se observa el archivo passwd de una de las máquinas en donde se evidencia que una de las máquinas de la red tiene dos usuarios: debianita y Juan, en el registro de trabajos se observa que antes de denegar el servicio al usuario Juan, éste podía imprimir efectivamente, en la parte posterior a este registro (arriba) puede verse la hora en la que el usuario Juan intentó realizar una impresión y ya tenía denegado el servicio.

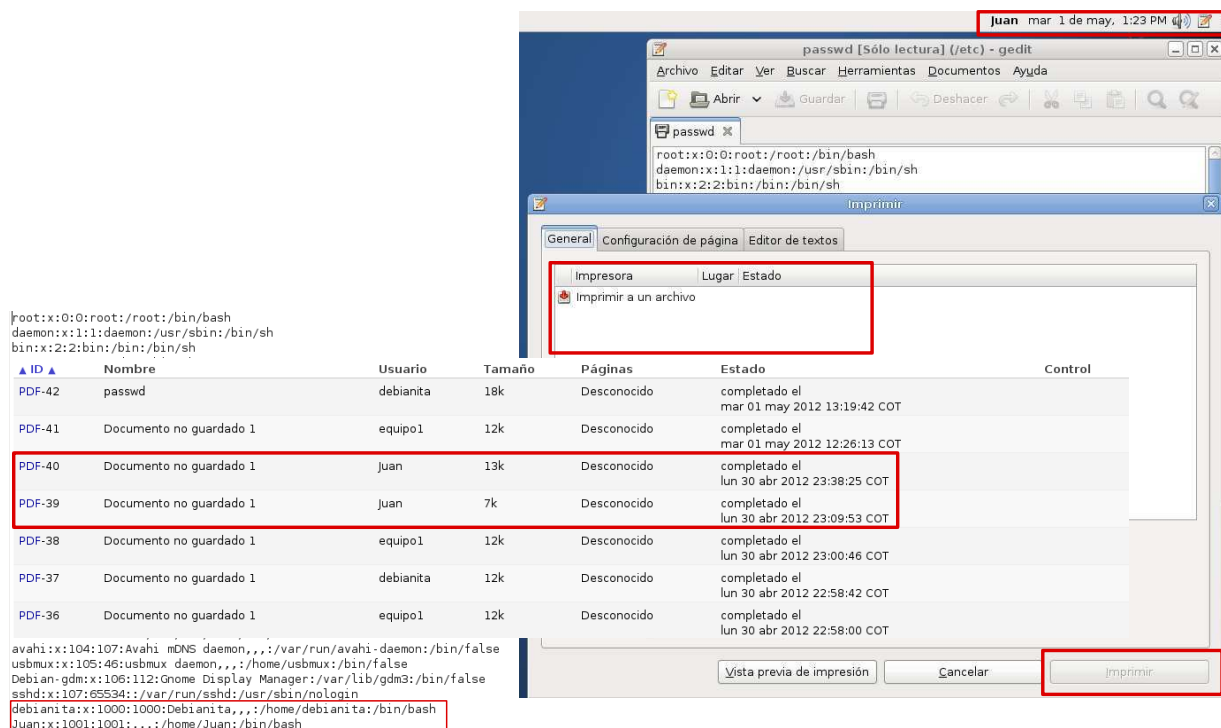


Figura 3: Comparativa del servicio pre - post Denegación al usuario Juan

3. Parte 3 Práctica SSH, SCP y SFTP:

Se desarrolló la práctica utilizando un servidor Debian y dos clientes, uno Debian y otro Canaima, las tres máquinas virtualizadas con VirtualBox.

- En un ordenador con GNU/Linux, instalar el servidor OpenSSH, comprobar su funcionamiento, haciendo pruebas de conexión desde la misma máquina y desde otras máquinas.

La instalación del sistema operativo en la máquina servidor se hizo teniendo en cuenta que deberá actuar como servidor SSH, en los clientes se hizo la respectiva instalación aunque en particular en Canaima GNU/Linux el servidor - cliente SSH esta instalado por defecto, la siguiente imagen muestra la conexión al servidor desde el cliente Canaima y desde el propio servidor.

```

root@canaima-popular:/home/equipol# ssh 192.168.1.4
The authenticity of host '192.168.1.4 (192.168.1.4)' can't be established.
RSA key fingerprint is 76:18:d4:4b:83:1f:d3:cb:0d:1d:86:f6:f8:2e:b5:28.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.1.4' (RSA) to the list of known hosts.
root@192.168.1.4's password:
Linux Servidor 2.6.32-5-686 #1 SMP Mon Mar 26 05:20:33 UTC 2012 i686

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Mon Apr 30 12:03:49 2012
-bash: warning: setlocale: LC_ALL: cannot change locale (es_VE.UTF-8)
root@Servidor:~#

```

Figura 4: Conexión SSH desde Canaima GNU/Linux

```

root@Servidor:/home/debianita# ssh Servidor
The authenticity of host 'servidor (127.0.1.1)' can't be established.
RSA key fingerprint is 76:18:d4:4b:83:1f:d3:cb:0d:1d:86:f6:f8:2e:b5:28.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'servidor' (RSA) to the list of known hosts.
root@servidor's password:
Linux Servidor 2.6.32-5-686 #1 SMP Mon Mar 26 05:20:33 UTC 2012 i686

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Tue May 1 14:37:17 2012 from 192.168.1.3
root@Servidor:~#

```

Figura 5: Conexión desde el mismo servidor SSH Debian GNU/Linux

- b) *Configurar el sistema para que el usuario pueda conectarse sin tener que entrar una contraseña, empleando una par de claves criptográficas (del criptosistema RSA) que también se deberán generar.*

En primer lugar se generan las claves RSA utilizando

```
# ssh-keygen
```

Luego la clave pública debe copiarse en el servidor ssh, para ello, desde el directorio donde se almace la clave pública se ejecuta

```
# ssh-copy-id -i id_rsa.pub 192.168.1.4
```

Las siguientes imágenes muestran la generación de las claves (privada y pública), la copia al servidor ssh de la clave pública, y la conexión del cliente al servidor utilizando la clave RSA.

```

root@canaima-popular:/home/equipol# ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/root/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /root/.ssh/id_rsa.
Your public key has been saved in /root/.ssh/id_rsa.pub.
The key fingerprint is:
b8:03:c9:a5:90:c9:6b:77:40:95:03:1f:e2:2b:4a:fe root@canaima-popular
The key's randomart image is:
+--[ RSA 2048]-----+
|      +oo.          |
|      . = oo.       |
|      = o o.        |
|      + * .         |
|      .+ B o S      |
| oo o o .           |
| .. o              |
| . .               |
| E                 |
+-----+
root@canaima-popular:/home/equipol# cd /root/.ssh
root@canaima-popular:~/ssh# ls
id_rsa id_rsa.pub known_hosts

```

Figura 6: Creación de claves RSA

```

root@canaima-popular:~/.ssh# ssh-copy-id -i id_rsa.pub 192.168.1.4
root@192.168.1.4's password:
bash: warning: setlocale: LC_ALL: cannot change locale (es_VE.UTF-8)
Now try logging into the machine, with "ssh '192.168.1.4'", and check in:

  .ssh/authorized_keys

to make sure we haven't added extra keys that you weren't expecting.
root@canaima-popular:~/.ssh# clear

```

Figura 7: Copia de la clave RSA pública al servidor SSH

```

root@canaima-popular:/home# ssh 192.168.1.4
Linux Servidor 2.6.32-5-686 #1 SMP Mon Mar 26 05:20:33 UTC 2012 i686

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Tue May 1 15:27:36 2012 from 192.168.1.3
-bash: warning: setlocale: LC_ALL: cannot change locale (es_VE.UTF-8)
root@Servidor:~#

```

Figura 8: Conexión utilizando clave RSA

- c) *Desde otro ordenador, verificar la conectividad mediante el protocolo SFTP y el protocolo SCP copiando ficheros en uno y otro sentido.*

Se crearon un par de archivos de texto plano en cada una de las máquinas para verificar la transferencia con cada uno de los protocolos, los resultados se muestran en las figuras 9 y 10. (Por alguna extraña razón al parcer \LaTeX no me permitió ubicar tantas figuras en la misma página, estoy consultando la razón.)

- d) *Entre los dos sistemas (SFTP y SCP) propuestos para compartir ficheros, decir cuál se aconseja utilizar y porqué (analizar que aspectos son los importantes por ejemplo no solamente tener en cuenta el protocolo y su velocidad sino también la gestión y administración de los archivos remotos.)*

Al ser el protocolo SFTP una "actualización" del protocolo FTP, es el protocolo que recomendaría si la transferencia y gestión de archivos es una tarea cotidiana ya que en comparación con el protocolo SCP (diseñado específicamente para transferir archivos), el protocolo SFTP cuenta con una interface de gestión de archivos con comando omólogos a los que se utilizan de manera local (cd, ls, etc) lo que permite contar con recursos más amplios a la hora de administrar archivos remotos, también cabe mencionar que es un protocolo de más transparente implementación desde sistemas no GNU, factor, que dado el contexto propuesto, debe tenerse en cuenta a la hora de elegir el protocolo de gestión y transferencia de archivos.

```

root@canaima-popular:/home/equipol/Documentos# scp Cliente_Servidor.txt 192.168.1.4:/home/debianita/Desktop
bash: warning: setlocale: LC_ALL: cannot change locale (es_VE.UTF-8)
Cliente_Servidor.txt                                100% 601      0.6KB/s   00:00
root@canaima-popular:/home/equipol/Documentos# scp 192.168.1.4:/home/debianita/Desktop/Servidor_Cliente.txt ./
bash: warning: setlocale: LC_ALL: cannot change locale (es_VE.UTF-8)
Servidor_Cliente.txt                                100% 529      0.5KB/s   00:00
root@canaima-popular:/home/equipol/Documentos# █

```

Figura 9: Copia de archivos usando SCP

```
connected to 192.168.1.4.
sftp> put /home/Juan/Desktop/Copia_SFTP_CS.txt /home/debianita/Desktop/
Uploading /home/Juan/Desktop/Copia_SFTP_CS.txt to /home/debianita/Desktop/Copia_SFTP_CS.txt
/home/Juan/Desktop/Copia_SFTP_CS.txt 100% 353 0.3KB/s 00:00
sftp> get /home/debianita/Desktop/Copia_SFTP_SC.txt /home/Juan/Desktop
Fetching /home/debianita/Desktop/Copia_SFTP_SC.txt to /home/Juan/Desktop/Copia_SFTP_SC.txt
/home/debianita/Desktop/Copia_SFTP_SC.txt 100% 361 0.4KB/s 00:00
sftp>
```

Figura 10: Copia a través de SFTP